

Application No. 10/534,067
Amendment dated October 21, 2009
Reply to Office Action of July 21, 2009

Docket No.: C3110.0001

AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to label Figure 1 as "Prior Art." No new matter has been added. A Replacement Sheet and Annotated Sheet are submitted for Figure 1.

REMARKS

Claims 1-21 are pending. Claim 1 is the only independent claim. Claims 1, 3, 7 and 21 have been amended. Figure 1 has been labeled Prior Art, as required in the Office Action.

Claims 3 and 7 were objected to because of punctuation issues. As shown above, these claims have been amended, without narrowing their scope, to conform with the punctuation requirements for U.S. patent claims. Withdrawal of the objection is respectfully requested.

Claim 21 was rejected under 35 U.S.C. § 112, second paragraph, as indefinite. As shown above, claim 21 has been amended, without narrowing its scope, to remove the objected to term “possibly.” Withdrawal of the rejection under Section 112 is respectfully requested.

Claims 1-16 and 19-21 were rejected under 35 U.S.C. § 102(e) over U.S. Patent 7,350,076 (Young et al.). Claims 17 and 18 were rejected under 5 U.S.C. § 103 over Young et al. in view of U.S. Patent 5,515,439 (Bantz et al.). Applicants submit that amended independent claim 1 is patentable over the cited art for at least the following reasons.

According to the amended claim 1, cryptography technology is utilized so that the wireless access point AP and the mobile terminal MT both have a certificate (e.g., a public key certificate) representing their respective identities. When the mobile terminal MT logs onto the wireless access point AP, using the claimed method, both the MT and AP send their respective certificates to a trusted third party—i.e., the authentication server AS. The authentication server AS authenticates the certificates of the wireless access point AP and the mobile terminal MT and notifies the certificate authentication result to the wireless access point AP and the mobile terminal MT. Then both the wireless access point AP and the mobile terminal MT can obtain the certificate authentication result of the other side so that the two way identity authentication between the wireless access point AP and the mobile terminal MT can be directly realized. As a result of the claimed method, legal mobile terminal accessing a legal accessing point can be guaranteed.

In the wireless local area network, due to the wireless characteristics of the transmission medium, the privacy of the wireless link telecommunication data must be guaranteed. To achieve this, according to claim 1, when the mobile terminal MT logs onto the wireless access point AP, it should be guaranteed that there is a shared secret key for conversation between each AP and each MT through the procedure of the negotiation thereof. Then the privacy of the conversion between the two parties during telecommunication can be guaranteed by using the secret key to protect the telecommunication data on the wireless link. Thus the negotiation of secret key for conversation has been defined in the amended claim 1.

Young et al. proposed the general solution (figure 3, lines 42-66 of column 5, lines 56-67 of column 9, lines 1-23 of column 10) as follows: before the first electronic device communicates with the second electronic device, the second electronic device is authenticated to the first electronic device, then the first electronic device is authenticated to the second electronic device so that the two way authentication between the two parties is realized and the secret key to be used by the two parties is negotiated. Finally, the authentication server still needs to authenticate the user's identity (the first electronic device) and only when the user passes the identification, the secure communication can be established. That is to say, the user can transmit and receive data secretly through the network.

Young et al. provides two embodiments to realize this technical solution. According to one of them (figure 4, lines 24-67 of column 10, column 11), the first electronic device is the user device while the second electronic device is the network device. The user device and the network device carry out two way authentication and secret key negotiation on the basis of pre-shared key. Then the central authentication server CAS realizes secret identity authentication of the user device. After the identity of the user is successfully authenticated, secret data communication will start between the user device and the network device.

In the second embodiment (figure 5, column 12 and lines 1-37 of column 13), the first electronic device is the user device, the second electronic device is the central authentication service CAS and the network device is only a relay station. The user device and the central authentication

server CAS realize two way authentications through the relay station relying on the EAP-TLS protocol and negotiate the master key. Finally, the central authentication server CAS transfers the negotiated master key to the network device through the secure channel pre-set between the network device and the central authentication server CAS (lines 52-56 of column 12). Then the central authentication server CAS accomplishes authentication of the user's identity. After the identification is successful, the user device and the network device can carry out secret data communication by using the secret key for conversation derived from the master key.

As understood by applicants, the user device, the network device and the central authentication server CAS in Young et al. are respectively regarded in the Office Action as corresponding to the mobile terminal, the wireless access point AP and the authentication server AS of the claims, respectively. However, claim 1 discloses a totally different technical solution compared with Young et al., for at least the following reasons.

(1) Process of the two-way authentication

In claim 1 when a mobile terminal MT logs on a wireless access point AP, the mobile terminal's certificate and the access point's certificate are transmitted to the trusted third party-- authentication server AS, to do the authentication work. In this manner, direct two way authentication between the mobile terminal MT and the wireless access point AP is realized.

In Young et al., as understood, a two-way (mutual) authentication process takes place between the first electronic device and the second electronic device without the third party taking part in (lines 1-10, column 10). After authentication to each other, the two parties find out whether the other one is legal and the two way authentication is accomplished.

In Young's first embodiment, the two way authentication process is realized directly between the user device and the network device based on the pre-shared key. This mode of authentication is suitable for small scaled wireless local area network (lines 24-30, column 10). In

Young's second embodiment, the two way authentication process takes place between the user device and the central authentication server CAS instead of the user device and the network device.

(2) Roles of the two-way authentication

In claim 1 the wireless access point AP, the mobile terminal MT and the authentication server AS all take roles in the process of two-way authentication and the three of them together achieve the authentication function. Therefore, claim 1 relates to a three roles-three entities architecture.

In Young et al. the first electronic device and the second electronic take roles in the two way authentication process, which belongs to a two roles-three entities architecture. In the first embodiment of Young et al., the user device and the network device takes roles in the authentication process while the central authentication server CAS does not participate the authentication procedure. In the second embodiment of Young et al., the user device and the central authentication server CAS take roles in the authentication process while the network device does not participate the authentication procedure and is only a relay device.

(3) Transmission of the trust relationship

In claim 1 the mobile terminal MT and the wireless access point AP authenticate each other through the authentication server AS. Therefore, the two way authentication between the mobile terminal MT and the wireless access point AP is directly achieved and the trust relationship between the mobile terminal MT and the wireless access point AP is directly established.

In Young et al., in the second embodiment, the central authentication server CAS secretly transfers its trust relationship (e.g. the negotiated master key) with the mobile terminal established during the two way authentication process to the network device through a secure channel pre-set between the network device and the central authentication server CAS, and the trust relationship between the mobile terminal MT and the wireless access point AP is indirectly

established. Therefore, transmission of the trust relationship on the network introduces security risks.

(4) Access control of the mobile terminal MT by the wireless access point AP

In claim 1 the wireless access point AP directly controls the mobile terminal MT to access according to the authentication result of the mobile terminal MT obtained by the wireless access point AP.

In Young et al., according to the identity authentication result of the user device obtained by the central authentication server CAS, the network controls the user device to access. Therefore, after the two way authentication process between the first electronic device and the second electronic device, further the identification of the user carried by the central authentication server CAS is still necessary. In this way, the complexity of the protocol is undoubtedly increased. Furthermore, it is necessary to transmit the identification result of the user from the central authentication server CAS to the network device through the secure channel pre-set between the network device and the central authentication server CAS. The transmission of the identification result on the network undoubtedly introduces the security risks.

(5) Secure channel

By virtue of the recited method of claim 1, it is not necessary to establish a secure channel between the wireless access point AP and the authentication server AS.

In Young et al., to the contrary, it is necessary to establish a secure channel between the network device and the central authentication server CAS for the transmission of the trust relationship and safe transfer of the identification result. The establishment of the secure channel makes the deployment of the network complex and hard to expand.

In summary, the method of claim 1 adopts a totally different technical solution to achieve safe communication in the wireless environment compared with Young et al. In particular, Young et al. fails to teach or even suggest the following technical features of claim 1:

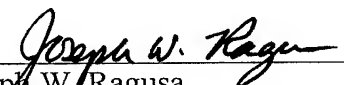
“wherein when a Mobile Terminal (MT) logs on a wireless Access Point (AP), a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transmitted to an Authentication Server (AS) and are authenticated through the Authentication Server (AS), then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned to the Access Point (AP) and the Mobile Terminal (MT) in order to achieve the direct two-way certificate authentication between said Mobile Terminal (MT) and Access Point (AP); and the Mobile Terminal (MT) and the Access Point (AP) perform negotiation of the secret key for conversation.”

For at least the foregoing reasons, amended claim 1 is believed clearly patentable over Young et al. The dependent claims are believed patentable for at least the same reasons as claim 1. The other references are not believed to remedy the abovementioned deficiencies of the cite art.

In view of the above amendments and remarks, applicants believe the pending application is in condition for allowance.

Dated: October 21, 2009

Respectfully submitted,

By 
Joseph W. Ragusa
Registration No.: 38,586
DICKSTEIN SHAPIRO LLP
1633 Broadway
New York, New York 10019-6708
(212) 277-6500
Attorney for Applicant

FPEL03150020

1/2

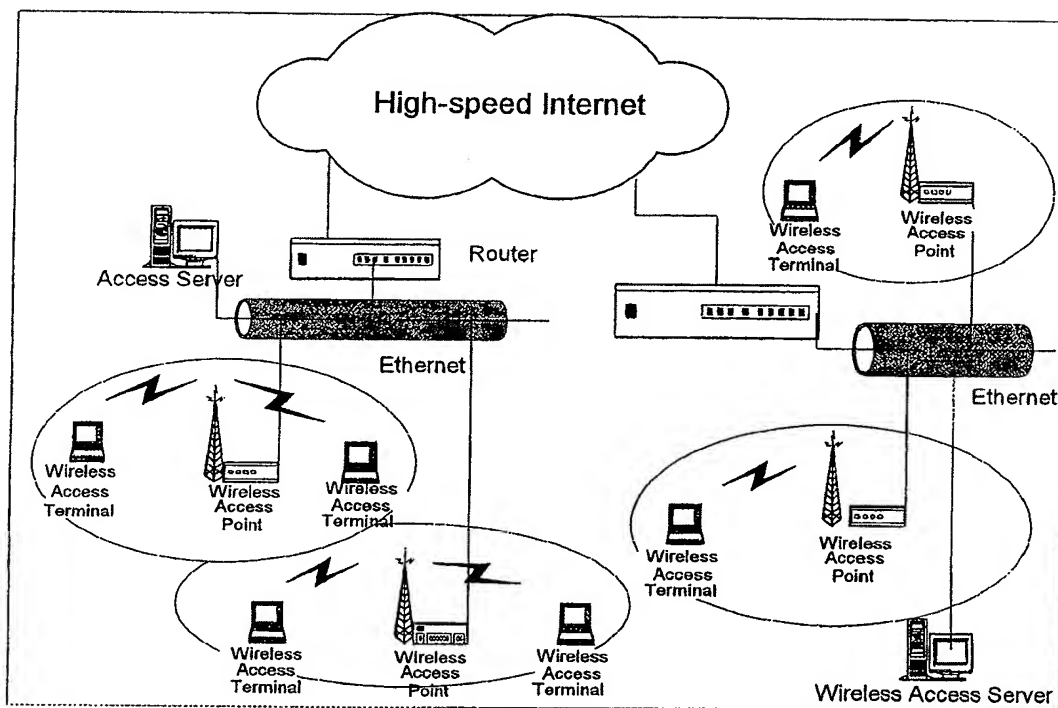


Fig. 1 Prior Art

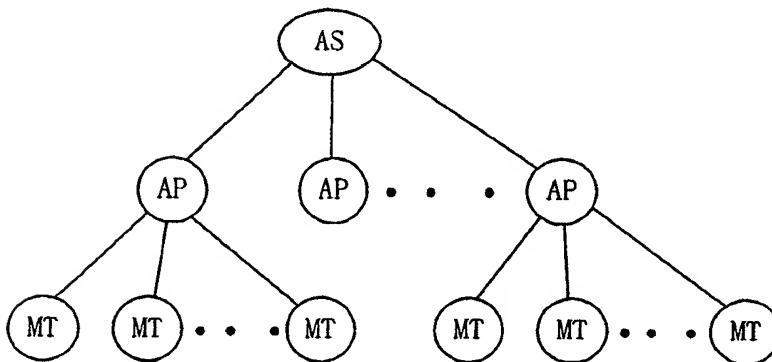


Fig. 2